7/9/03

decrypting the session key at the intermediary;

decrypting, at the intermediary, the encrypted data using the session key; and

inspecting the data in route between the internal and external clients.

20. (Unchanged) In a network system in which an encrypted data stream is transferred over a network between two endpoints and via an intermediary, the data stream being encrypted using a session key known to both endpoints, computer-readable media at one of the endpoints and at the intermediary storing computer-executable instructions for:

securely transferring the session key from one of the endpoints to an intermediary having access to the encrypted data stream;

decrypting the encrypted data stream at the intermediary using the session key; and

inspecting the data stream following decryption.

REMARKS

Applicant respectfully requests reconsideration and allowance of the subject application. Claims 1-20 are pending.

35 U.S.C. §112

The Examiner has withdrawn the 35 U.S.C. §112 rejection of claims 3, 7, 8-11 of the previous office action.

35 U.S.C. §101

The Examiner has withdrawn the 35 U.S.C. §101 rejection of claims 12-18 of the previous office action.

35 U.S.C. §102

Claims 1 and 4 remain rejected under 35 U.S.C. §102 as being anticipated by U.S. Patent 5,835,726 to Shwed et al (Shwed). Applicants respectfully traverse the rejection.

The invention concerns a network architecture in which two endpoints communicate via a virtual private network (VPN) on an otherwise public network, such as the Internet, and an intermediary is permitted to inspect the data communication in a secure and trusted manner.

In one implementation, the network architecture has an external client and an internal client that exchange encrypted data over a network. The internal client is coupled to the network via a network access point, such as a firewall/proxy server. All three participants have their own pair of public/private keys. An independent key server holds the public keys for all three participants.

The external and internal clients establish a virtual private network by negotiating a session key used to encrypt data being exchanged between them. Initially, only the clients know the session key, and not the firewall. To grant the firewall trusted access to the data stream on the VPN, the internal client securely transfers the session key to the firewall. The internal client requests and receives the firewall's public key from the key server and encrypts the session key using the firewall's public key. The internal client then signs the encrypted key by encrypting it using the internal client's private key.

The firewall authenticates the signature by decrypting the message using the internal client's public key (obtained from the key server or directly from the internal computer). The firewall then decrypts the session key using its own private key. If the dual decryption yields a valid key, the firewall is assured that the session key was sent by the internal client and was not subsequently altered or tampered with in route.

Once the session key is transferred, the firewall is able to decrypt the data stream on the VPN. The firewall can now un-intrusively inspect the data stream in a manner that is transparent to the external and internal clients. The claims capture this architecture and new technology.

Fig. 2 of the present application is representative of the invention and is reproduced below.

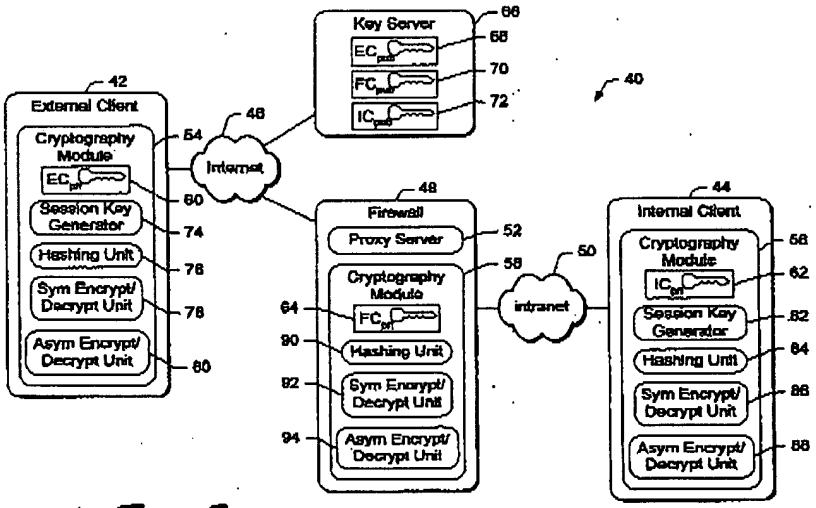

Fig. 2

Claim 1 for example recites a "method for inspecting an encrypted data stream being transferred over a network between two endpoints, the data stream being encrypted using a session key known to both endpoints, the method comprising:

securely transferring the session key from one of the endpoints to an intermediary having access to the encrypted data stream;

decrypting the encrypted data stream at the intermediary using the session key; and

inspecting the data stream following decryption."

The method of claim 1 provides for an establishment of a virtual private network (VPN) between two computers (endpoints) where the computers (endpoints) engage in key negotiation process to negotiate a session key (see specification page 9, lines 11-13). With the session key, the endpoints (internal and external clients) are able to encrypt messages and begin an encrypted communication session directly with one another (see specification page 9, lines 11-17, Fig. 2). Once the session key is created, one of the endpoints is able to securely share the key with an intermediary to permit trusted inspection. All three participants have their own pair of public/private keys (see specification page 7, lines 11-17).

The method of claim 1 is not disclosed by Shwed. Shwed shows host 1 and host 2 computers (also referred to by the Examiner as endpoints) connected to respective private networks. Host 1 and Host 2 are secured through respective firewalls. The firewalls connect to one another by way of a public network. See Shwed, col 14, lines 19-39, Fig. 16. Host 1 and Host 2 do not directly communicate with one another.

Fig. 16 of Shwed is redrawn below.

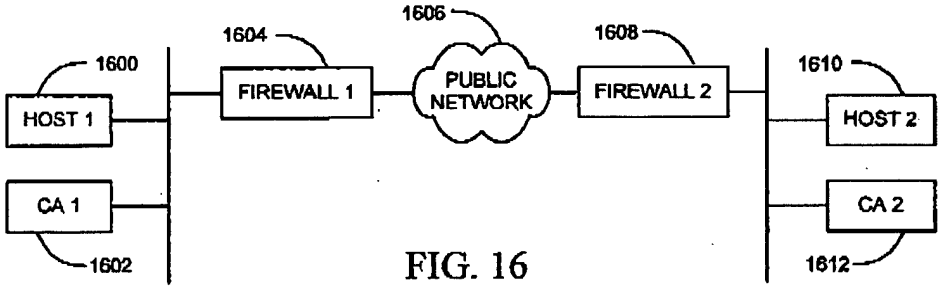

FIG. 16

Shwed does not teach or disclose that Host1 and Host2, one of which is considered an endpoint in Shwed, as knowing a session key. An element of the claims as recited in claim 1 is "a session key known to both endpoints." The Examiner has pointed to teachings in Shwed that show a session key that is known by a firewall or an outside client. In Shwed a session key is generated by the non-initiator firewall also called the destination and is sent encrypted to the initiator firewall (Shwed at col. 15, lines 33-35). Shwed does not teach or disclose that either Host 1 or Host 2 would know the session key, in view of the fact that Host1 or Host 2 do not decrypt or encrypt data. As discussed Shwed makes particular mention that communication to and from Host 1 and Host 2 are never encrypted, and does not teach or disclose that either Host 1 or Host 2 would know a session key. Either Host 1 or Host 2 is viewed as an endpoint the teaching of Shwed, however, in any configuration taught by Shwed neither Host 1 nor Host 2 will know a session key.

The Examiner argues that "Shwed desires that the communications between Host 1 and Host 2 be secured" referring to Shwed at col. 14, lines 40-41. However, this security is only performed through firewall 1 and firewall 2. In other words, secured communication disclosed or taught by Shwed is from firewall to firewall, or in other cases a client (host) to a firewall. "As stated previously,